

COPY OF PAPERS
ORIGINALLY FILED

#7
BJ
5-29-02
2682

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of

BREITBACH et al.

Examiner:

Serial No.: 09/936,834

Art Unit:

Date Filed: September 17, 2001

Docket No.: P-44 MG

PCT International Application No.: PCT/DE00/00792

For: Method for Using Standardized Bank Services via the Internet

Director of Patents, U.S. Patent Office
Washington, D.C. 20231

RECEIVED
MAY 17 2002
Technology Center 2600

SUBMISSION OF PRIORITY DOCUMENT

SIR:

Applicants, through their attorneys of record, submit a certified copy of the priority document in this patent application, German Patent No. 199 11 782.9 filed March 17, 1999, entitled "Verfahren zur Nutzung von standardisierten Bankdienstleistungen uber Mobilfunk."

U.S. Patent Application of BREITBACH et al.
Serial No.: 09/936,834 – Docket No.: P-44 MG

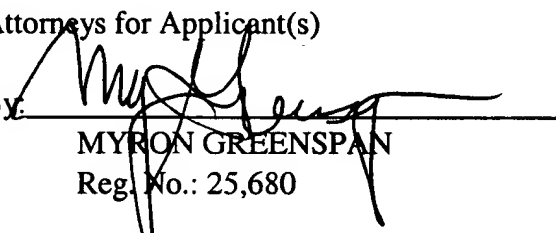
Applicants and their undersigned attorney of record respectfully request that the Examiner review this document and make it of record in any patent to issue on this application.

Dated: May 3, 2002

Lackenbach Siegel, LLP
One Chase Road
Scarsdale, NY 10583
Telephone: 914 723 4300
MG/as

Respectfully submitted,

LACKENBACH SIEGEL, LLP
Attorneys for Applicant(s)

By: 
MYRON GREENSPAN
Reg. No.: 25,680

Certificate of Deposit by Mail

I hereby certify that this correspondence is being filed by depositing same in an envelope stamped first-class mail, addressed to the Director of Patents, U.S. Patent Office, Washington, D.C. 20231, in a duly marked U.S. Postal Service drop box, with appropriate postage, on the following date:

Myron Greenspan

Attorney

Signature

May 3, 2002

Date

Applicant hereby petitions that any and all extensions of time of the term necessary to render this response timely be granted. COSTS FOR SUCH EXTENSION(S) AND/OR ANY OTHER FEE DUE WITH THIS FEE DUE WITH THIS PAPER THAT ARE NOT FULLY COVERED BY AN ENCLOSED CHECK MAY BE CHARGED TO DEPOSIT ACCOUNT #10-0100.

BUNDESREPUBLIK DEUTSCHLAND



**CERTIFIED COPY OF
PRIORITY DOCUMENT**

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

RECEIVED

MAY 17 2002

Technology Center 2600

Aktenzeichen:	199 11 782.9
Anmeldetag:	17. März 1999
Anmelder/Inhaber:	DeTeMobil Deutsche Telekom MobilNet GmbH, Bonn/DE
Bezeichnung:	Verfahren zur Nutzung von standardisierten Bank- dienstleistungen über Mobilfunk
IPC:	H 04 L, H 04 Q

**Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ur-
sprünglichen Unterlagen dieser Patentanmeldung.**

München, den 04. Oktober 2001
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hiermit...

DeTeMobil Deutsche Telekom MobilNet GmbH, Bonn

Verfahren zur Nutzung von standardisierten Bankdienstleistungen über Mobilfunk

Die Erfindung betrifft ein Verfahren zur Nutzung von standardisierten Bankdienstleistungen über Mobilfunk.

Für die Inanspruchnahme von Bankdienstleistungen werden in zunehmendem Maß papierlose, bequeme Wege der Einreichung und Abfrage nachgefragt. Bankenseitig wird diese Entwicklung wegen der damit erzielbaren Rationalisierungseffekte gefördert und es wurde dazu von der deutschen Kreditwirtschaft ein Verfahren zum bankübergreifenden Homebanking durch den Einsatz von z.B. einem Personal Computer (PC) und einem Festnetzmodem, entwickelt. Diese als HBCI (Home Banking Computer Interface) bezeichnete Verfahren beruht auf einer kryptographischen Ende-zu-Ende Verschlüsselung zwischen einem Personal Computer (Client) auf Kundenseite und dem Bankserver (vgl. Homebanking Computer Interface, Schnittstellenspezifikation, Version 2.0.1. vom 02.02.1998). Die in Deutschland mit unter 10% recht geringe Penetration von PC-Online-Zugängen stellt hier allerdings zunächst ein Hemmnis dar.

Der Mobilfunk mit ca. 15 Millionen Kunden und hohen Wachstumsraten ist erheblich weiter verbreitet. Hier liegt ein möglicher Schlüssel für einen massenmarktfähigen elektronischen Zugang zu Banktransaktionen. Hinzu kommt für den Kunden die Möglichkeit, auch mobil Zugang zu Bankgeschäften zu erlangen.

Der HBCI-Standard ist in der deutschen Bankenwelt als Plattform für Homebanking vorgesehen. Es bietet sich an, auf diesen Standard auch im Kontext von

mobildfunkgestütztem Banking aufzusetzen. Leider ist das für das Internet konzipierte HBCI-Protokoll zu umfangreich für eine direkte Abbildung auf die heutige GSM-Mobildfunkwelt. Dies betrifft sowohl die für die Datenübertragung notwendige Bandbreite, als auch die benötigte Speicherkapazität und Rechenleistung auf Seite des Mobildfunkteilnehmers bzw. dessen Mobilstation.

Es ist Aufgabe der Erfindung, ein Verfahren vorzuschlagen, welches die Nutzung von standardisierten Bankdienstleistungen über Mobildfunk erlaubt, wobei herkömmliche Mobilstationen ohne Zusatzgeräte als kundenseitige HBCI-Plattform eingesetzt werden können.

Diese Aufgabe wird durch die in Anspruch 1 angegebenen Merkmale gelöst.

Grundidee dieser Erfindung ist die Verteilung des kundenseitigen HBCI-Systems auf zwei Komponenten - die in der Mobilstation verwendete SIM-Karte (Teilnehmeridentitätsmodul) und einen HBCI-Gateway.

Es werden dazu zwei Übertragungsstrecken gebildet, erstens zwischen SIM-Karte und HBCI-Gateway und zweitens zwischen HBCI-Gateway und Bankserver. Auf beiden Teilstrecken wird eine kryptographische Sicherung realisiert.

Der HBCI-Gateway wird also in den Übermittlungsweg eingefügt. Dieser entpackt das HBCI-Protokoll und wandelt den Protokollablauf derart, dass eine Verträglichkeit mit der GSM-SIM-Karte und dem GSM-Netzstandard erwirkt wird. Der HBCI-Gateway schliesslich tauscht das gewandelte Protokoll mit einer kundenseitig verwendeten SIM-Karte aus. Es erfolgt demnach eine Transformation zwischen dem bankenseitig verwendeten HBCI und einem auf der Mobildfunkseite verwendeten Übertragungsprotokoll. Die Aufgabe des HBCI-Gateways ist im wesentlichen die Reduktion der zu übertragenden Daten auf ein GSM-kompatibles Maß.

Als Trägerdienst für den Informationsaustausch zwischen HBCI-Gateway und Mobildfunkteilnehmer kann z.B. der Short Message Service oder GPRS dienen.

Aus Sicht des Bankservers wird komplett ein standardkonformes HBCI-Protokoll genutzt, wobei zwischen Bankserver und HBCI-Gateway das durch HBCI definierte Sicherheitsprotokoll Anwendung findet. Zwischen HBCI-Gateway und SIM-Karte wird ein anderes Sicherheitsprotokoll verwendet. Dieses entspricht einem vom Datenumfang her reduzierten, aber sicherheitstechnisch HBCI äquivalenten Protokoll.

Anstelle des beim online-banking üblichen PCs übernimmt nun die SIM-Chipkarte die Funktionen des Kundensystems, sowohl was den Benutzerdialog, als auch was die Sicherheitsfunktionen angeht. Ermöglicht wird dies durch eine neue, standardisierte Technologie mit Namen SAT (SIM Application Toolkit), welcher es der Mobilfunk-Chipkarte (SIM-Karte) erlaubt, die Rolle der Dienststeuerung wahrzunehmen.

Sowohl die SIM-Karte als auch der Bankrechner kommuniziert jeweils direkt ausschließlich mit dem HBCI- Gateway; dieser nimmt also eine Proxy-Funktion, d.h. eine stellvertretende Funktion des jeweiligen Gegenübers wahr.

Die erwähnte Transformation bringt auch eine Transformation der verwendeten Sicherheitsmechanismen mit sich; während zwischen dem Gateway und der Bankenwelt das HBCI-Protokoll angewendet wird, wird GSM-seitig ein eigenes Sicherheitsprotokoll verwendet.

In einer bevorzugten Weiterbildung der Erfindung ist vorgesehen, dass ein Verfahren zur Anwendung kommt, das es ermöglicht, kryptographische Schlüssel nach der SIM-Kartenpersonalisierung sicher in der SIM-Karte zu generieren und zu speichern. Hierzu wird vom HBCI-Gateway bzw. der Bank ein spezieller PIN Brief erzeugt. Die Eingabe der PIN am Mobiltelefon generiert den kundenspezifischen Schlüssel in der SIM-Karte

Auf diese Weise wird ein sicherer, verschlüsselter Kommunikationsweg zwischen HBCI-Gateway und SIM-Karte ohne Gefährdung durch „man in the middle“ Attacken, z.B. durch den Netzbetreiber, aufgebaut.

Nachfolgend wird die Erfindung anhand eines Ausführungsbeispiels unter Bezugnahme auf mehrere Zeichnungsfiguren erläutert.

Dabei gehen aus den Zeichnungen und ihrer Beschreibung weitere Merkmale und Vorteile der Erfindung hervor.

Figur 1 zeigt schematisch die erfindungsgemäss für die Bankdienstleistungen über Mobilfunk benötigten Einrichtungen.

Figur 2 zeigt beispielhaft ein Ablaufdiagramm für die erstmalige Freischaltung der Bankdienstleistungen über online-Subscription.

Das folgende Ausführungsbeispiel basiert auf der RDH-Variante für HBCI und auf einer symmetrischen Triple-DES Lösung (DES = Data Encryption Standard) auf GSM-Seite.

In Figur 1 sind schematisch die am beschriebenen Verfahren beteiligten Einrichtungen gezeigt. Es ist eine Mobilstation 1, bestehend aus Endgerät 2 und Teilnehmeridentitätsmodul 3 (SIM) gezeigt, mittels welcher ein Mobilfunkteilnehmer mit dem Mobilfunknetz, dargestellt als Basisstation 6 über die Luftschnittstelle 5 kommunizieren kann.

Für die Nutzung von Dienstleistungen muss der Mobilfunkteilnehmer über das Mobilfunknetz mit seiner Bank 9 in Verbindung treten. Die Bankdienstleistung werden über einen speziellen Bankserver 10 abgewickelt, welcher ein nach dem HBCI-Standard definiertes Protokoll zur elektronischen Kommunikation mit dem Teilnehmer benutzt.

Auf der GSM-Luftschnittstelle 5 kommt die GSM-Standardverschlüsselung 12 zur Anwendung. Darüber liegt auf Applikationsebene eine Triple-DES Verschlüsselung 11, welche die Strecke zwischen SIM-Karte 3 und HBCI-Gateway 7 absichert. Die Strecke zwischen HBCI-Gateway 7 und Bank 9 bzw. Bankserver 10 unterliegt dem Standard-HBCI-Protokoll in der RDH-Variante, wobei ein asymmetrisches RSA-Verschlüsselungsverfahren 13 angewendet wird.

Da der HBCI-Gateway 7 sicherheitsrelevante Funktionen wahrnimmt, besteht die Möglichkeit, daß er direkt in den Bankrechenzentren betrieben wird. Die Einrichtung des HBCI-Gateways beim jeweiligen Netzbetreiber ist ebenfalls möglich.

Zur Sicherung der Strecke zwischen HBCI-Gateway 7 und SIM-Karte 3 ist es erforderlich, einen geheimen Schlüssel Ksms zwischen dem Gateway 7 und der SIM-Karte 3 zu definieren. Um die Geheimhaltung des Schlüssels Ksms absolut sicherzustellen, wird ein Verfahren vorgeschlagen, bei welchem die Bank per PIN-Brief eine Initialisierungs-PIN an den Mobilfunkteilnehmer versendet, welchen der Teilnehmer einmalig am Mobiltelefon 2 eingibt. In der SIM 3 sowie im HBCI-Gateway 7 wird daraus mittels eines geeigneten Algorithmus der Schlüssel Ksms abgeleitet. Damit ist sichergestellt, daß Dritte keine Kenntnis dieses Schlüssels haben. Weiter unten wird das Sicherungsverfahren ausführlich dargestellt.

Dem Teilnehmer können z.B. die Geschäftsvorfälle Kontostandsabfrage, letzte Umsätze und Überweisungsauftrag angeboten werden. In jedem Fall erfolgt eine Verschlüsselung der Nachrichten mit Ksms.

Aktionen werden üblicherweise vom Nutzer über die Bedienersteuerung des Mobiltelefons 2 angestoßen.

Dazu kann zum Beispiel von der SIM-Karte 3 ein eigener Menüpunkt z.B. "Mobile Banking" am Endgerät eingestellt werden. Wird der eingerichtete Menüpunkt angewählt, können z.B. die Unterpunkte "Kontostand", "Umsätze", "Überweisung" und "Konfiguration" angeboten werden.

Aufgrund dessen, dass die begrenzten Möglichkeiten einer Mobiltelefon-Tastatur nach einer optimierten Benutzerführung verlangen, kann als Option vorgesehen sein,

dass insbesondere die eigene Bankverbindung in der SIM-Karte 3 abgelegt ist, so daß diese nur einmalig eingegeben werden muß.

Um sicherzustellen, daß Unbefugte nicht in die Lage versetzt werden, Banktransaktionen zu veranlassen, sollte bei jeder Transaktionsanforderung eine lokale PIN abgefragt werden. Diese PIN wird lokal von der Karte verwaltet.

Nachfolgend wird ein Beispiel für den Ablauf der Subskription des Teilnehmers angegeben.

- Die Freischaltung des Banking-Dienstes erfolgt gemäß Darstellung in Figur 2 durch Anwahl eines eingerichteten Menüpunktes "Konfiguration" (s.o.); hierauf werden in einem nächsten Schritt die BLZ und Konto-Nummern der eigenen Konten abgefragt, sowie Initialisierungs-PIN und lokale PIN für die Bankanwendung. Die Daten der eigenen Bankverbindungen werden auf der Karte abgespeichert. In einem weiteren Schritt wird aus der Initialisierungs-PIN und einem aus einem Masterschlüssel abgeleiteten Initialisierungsschlüssel KIV von der Karte ein Schlüssel Ksms zur Sicherung der Kommunikation zwischen HBCI-GSM-Gateway und SIM-Karte berechnet. Die Abfrage der lokalen (Karten-) PIN dient dem Schutz gegen unauthorisierte Subskriptionsversuche.
- Nach der Berechnung von Ksms meldet die SIM-Karte dem HBCI-Gateway den Subskriptionswunsch. Hierauf erfolgt die lokale Schlüsselgenerierung am HBCI-Gateway sowie der Erstdialog mit dem HBCI-Bankensystem. Ferner sendet der HBCI-Gateway eine Nachricht zur Karte, welche das Anpassen des Bankmenü-Titels und das vollständige Aktivieren der Applikation bewirkt.

Sicherheit

Eine sehr wichtiges Merkmal des beschriebenen Verfahrens ist die Sicherheit. Ziel des Sicherheitskonzeptes ist vor allem, einen Mißbrauch zu verhindern (Authentifikation des Kunden). Desweiteren ist es wichtig, die Vertraulichkeit der übertragenen Daten zu gewährleisten (Verschlüsselung der Übertragung). Beide Anforderungen werden mittels kryptographischer Verfahren realisiert.

Sicherheitsbereiche

Die gesamte Strecke vom Mobiltelefon 1 des Kunden bis zum HBCI-Server 10 der Bank ist in zwei Sicherheitsbereiche aufgegliedert. Der erste Bereich erstreckt sich vom der SAT-SIM-Karte 3 bis zum HBCI-Gateway 7. Die Strecke vom HBCI-Gateway 7 zum Bankenserver 10 bildet den zweiten Sicherheitsbereich.

Sicherheitsbereich 1: SAT-SIM zu HBCI-Gateway

Die Sicherheitsfunktionen dieses Bereiches werden im wesentlichen durch Vergabe und Verwendung eines speziellen Schlüssels Ksms bestimmt. Mit diesem 128 Bit langen Triple-DES Schlüssel 11 werden alle zwischen SAT-SIM 3 und HBCI-Gateway 7 ausgetauschten Nachrichten verschlüsselt und signiert.

Der Ksms sichert die Verbindung von der SIM 3 bis zum HBCI-Gateway 7. Der Ksms authentifiziert sowohl den Teilnehmer als auch das HBCI-Gateway und wird auch zur Verschlüsselung dieser Strecke verwendet. Der Ksms ist ein spezifischer Schlüssel der Bankenapplikation und bleibt dem Netzbetreiber verborgen. Um dies zu gewährleisten, wird z.B. folgendes Verfahren zur Erzeugung angewandt:

Bei der Kartenpersonalisierung wird vom Netzbetreiber zusammen mit der Bankenapplikation ein KIV zur Erzeugung der kundenspezifischen Ksms auf alle Karten aufgebracht. Der KIV wird mit Hilfe eines Masterschlüssels und einer SIM-Kartenindividuellen Zahl erzeugt. Der Teilnehmer erhält vor Subskription des Dienstes die Daten seiner Bank inklusive einer 20-stelligen PIN. Bei der Initialisierung der SAT-Applikation (online-Subskription) wird aus der PIN mit Hilfe des KIV der eigentliche Kundenschlüssel Ksms erzeugt (verschlüsseln der PIN, der Bankleitzahl und der Kontonummer per Triple-DES mit KIV als Schlüssel).

Zur Erzeugung des Ksms im HBCI-Gateway 7 muß die PIN auch zum Gateway-Betreiber weitergereicht werden. Optional bietet sich die Erzeugung der PIN am HBCI-Gateway und die Weitergabe an die Bank an.

Die Authentifikation zwischen Teilnehmer und HBCI-Gateway erfolgt durch Wissen über die schriftlich ausgetauschte PIN. Zwischen Netzbetreiber und HBCI-Gateway-Betreiber muß zusätzlich ein Masterkey zur Erzeugung der KIV's ausgetauscht werden. Dieser Masterkey authentifiziert damit zusätzlich das HBCI-Gateway.

Optional kann darüber hinaus noch eine zusätzliche Authentifikation des Kunden über die Kennung seines Mobilanschlusses erfolgen:

Es kann beim HBCI-Gateway die Auswertung der Calling-Line-Identification (CLI) der versendeten SAT-SIM erfolgen. Dazu muß die Mobilfunkrufnummer des Kunden im HBCI-Gateway verwaltet werden.

Sicherheitsbereich 2: HBCI-Gateway zum Kreditinstitutsystem

Auf der Schnittstelle vom HBCI-Gateway 7 zur Bank 9 kommt ein unmodifiziertes HBCI-Protokoll zur Anwendung. In der hier dargestellten Ausgestaltung kommt die RDH-Variante zum Einsatz. Im Modell der HBCI-Spezifikation stellt das HBCI-Gateway das Kundensystem dar. Auf dem HBCI-Gateway sind die öffentlichen und privaten Signier- und Chiffrierschlüssel für jeden Kunden gespeichert.

Der Mechanismus der Authentifikation der öffentlichen Kunden- sowie Bankenschlüssel muß in einer vertraglichen Regelung zwischen Betreiber des HBCI-Gateways 7 und dem Betreiber des Bankenservers 10 erfolgen. Sollte kein implizites Vertrauensverhältnis zwischen diesen Parteien bestehen, können Ini-Briefe oder auch Zertifikate eingesetzt werden.

Die nachfolgende Tabelle gibt eine Übersicht über die im Verfahren verwendeten Schlüssel

Schlüssel	Verwendung	Generierung	Aufbewahrungsorte	Kenntnis durch
Ki	GSM-Authentisierung Luftschnittstelle	Netzbetreiber bei Kartenpersonalisierung	SIM, Authentication Center Netz- betreiber	Netzbetreiber
Kc	GSM Verschlüsselung Luftschnittstelle	Netz + SIM bei Verbindungsaufbau	Mobiltelefon + GSM-Netz	Netzbetreiber
CKpub	HBCI public key (Verschlüsselung) des Kunden	HBCI-Gateway bei Subskription	HBCI-Gateway, Bank	Gateway- Betreiber, Bank

CKpriv	HBCI private key (Verschlüsselung) des Kunden	HBCI-Gateway bei Subskription	HBCI-Gateway	Gateway- Betreiber
AKpub	HBCI public key (Authentifikation) des Kunden	HBCI-Gateway bei Subskription	HBCI-Gateway, Bank	Gateway- Betreiber
AKpriv	HBCI private key (Authentifikation) des Kunden	HBCI-Gateway bei Subskription	HBCI-Gateway	Gateway- Betreiber
CBpub	HBCI public key (Verschlüsselung) der Bank		Bank, HBCI-Gateway	Gateway- Betreiber, Bank
CBpriv	HBCI private key (Verschlüsselung) der Bank		Bank	Bank
ABpub	HBCI public key (Authentifikation) der Bank		Bank, HBCI-Gateway	Gateway- Betreiber, Bank
ABpriv	HBCI private key (Authentifikation) der Bank		Bank	Bank
KIV	Initialisierungs- schlüssel	Netzbetreiber	SIM-Karte	SIM-Karte, HBCI-Gateway
Ksms	Verschlüsselung und Authentifikation SAT-SIM zum Gateway	HBCI-Gateway vor Subskription sowie SAT-SIM bei Subskription	HBCI-Gateway, SAT-SIM	Gateway- Betreiber, indirekt auch Kunde

Das vorgeschlagene Verfahren bietet ein hohes Sicherheitsniveau. Die beteiligten technischen Komponenten (SIM, Mobiltelefon, HBCI-Gateway) sind weitaus weniger anfällig gegen Mißbrauch als etwa ein Personal Computer. Aus Sicht des Teilnehmers wird mit dem vorliegenden technischen Konzept ein neuartiger Dienst angeboten, welcher mit einem hohen Sicherheitsstandard einhergeht.

Patentansprüche

1. Verfahren zur Nutzung von standardisierten Bankdienstleistungen über Mobilfunk, wobei die Datenübertragung zwischen einem Bankserver und einer Mobilstation auf dem HBCI-Übertragungsverfahren aufbaut, dadurch gekennzeichnet, dass ein HBCI-Gateway in den Übermittlungsweg zwischen dem Bankserver und der Mobilstation geschaltet wird; der eine Transformation zwischen dem bankenseitig verwendeten HBCI-Übertragungsverfahren und einem auf der Mobilfunkseite verwendeten Übertragungsverfahren vornimmt.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine Aufspaltung des kundenseitigen HBCI-Systems in zwei Komponenten, die SIM-Karte der Mobilstation und den HBCI-Gateway, erfolgt.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass zwei Übertragungsstrecken gebildet werden, erstens zwischen SIM-Karte und HBCI-Gateway und zweitens zwischen HBCI-Gateway und Bankserver.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das HBCI-Protokoll vom HBCI-Gateway entpackt und dessen Protokollablauf derart umgewandelt wird, dass eine Verträglichkeit mit der GSM-SIM-Karte und dem GSM-Netz erwirkt wird so dass ein Austausch des gewandelten Protokolls mit der SIM-Karte möglich ist.
5. Verfahren nach einem der Ansprüche 1 bis 4, dass als Trägerdienst für den Informationsaustausch zwischen HBCI-Gateway und Mobilstation ein GSM Datenübertragungsdienst, insbesondere der Short Message Service, GPRS oder USSD dient.

6. Verfahren nach einem der Ansprüche 1 bis 5, dass auf beiden Teilstrecken eine kryptographische Sicherung realisiert wird.
7. Verfahren nach einem der Ansprüche 1 bis 6, dass zwischen Bankserver und HBCI-Gateway das durch HBCI definierte Sicherheitsprotokoll Anwendung findet und zwischen HBCI-Gateway und SIM-Karte ein zweites Sicherheitsprotokoll verwendet wird.
8. Verfahren nach einem der Ansprüche 1 bis 7, dass das zweite Sicherheitsprotokoll einem vom Datenumfang her reduzierten aber sicherheitstechnisch HBCI äquivalenten Protokoll entspricht.
9. Verfahren nach einem der Ansprüche 1 bis 8, dass ein kryptographischer, teilnehmerspezifischer Schlüssel (Ksms) zur Verwendung im zweiten Sicherheitsprotokoll nach der regulären SIM-Kartenpersonalisierung sicher in der SIM-Karte generiert und gespeichert wird.
10. Verfahren nach einem der Ansprüche 1 bis 9, dass die Generierung des teilnehmerspezifischen Schlüssels (Ksms) in der SIM-Karte durch Eingabe einer Initialisierungs-PIN am Mobiltelefon generiert wird.
11. Verfahren nach einem der Ansprüche 1 bis 10, daß die PIN zur Generierung des Schlüssels (Ksms) dem Teilnehmer durch die Bank per PIN-Brief mitgeteilt wird.
12. Verfahren nach einem der Ansprüche 1 bis 11, dass bei der Kartenpersonalisierung vom Mobilfunknetzbetreiber zusammen mit der Bankenapplikation ein aus einem Masterschlüssel und einer SIM-Kartenindividuellen Zahl abgeleiteter Initialisierungsschlüssel KIV, zur Erzeugung der teilnehmerspezifischen Ksms auf alle SIM-Karten aufgebracht wird.

13. Verfahren nach einem der Ansprüche 1 bis 12, dass der Teilnehmer vor Subskription des Dienstes die Daten seiner Bank inklusive einer Initialisierungs-PIN erhält.
14. Verfahren nach einem der Ansprüche 1 bis 13, dass bei der Initialisierung der Applikation, d.h. bei Subscription aus der Initialisierungs-PIN mit Hilfe des KIV der Schlüssel Ksms unter Verwendung der lokalen PIN, der Bankleitzahl und der Kontonummer per Triple-DES erzeugt wird.
15. Verfahren nach einem der Ansprüche 1 bis 14, dass zur Erzeugung des Ksms im HBCI-Gateway die Initialisierungs-PIN zum Gateway-Betreiber weitergereicht wird.
16. Verfahren nach einem der Ansprüche 1 bis 14, dass die Erzeugung der Initialisierungs-PIN am HBCI-Gateway erfolgt und dieser an die Bank weitergeleitet wird.
17. Verfahren nach einem der Ansprüche 1 bis 16, dass die Authentifikation der beiden beteiligten Stellen, Mobilfunkteilnehmer und HBCI-Gateway, durch Wissen über die schriftlich ausgetauschte Initialisierungs-PIN erfolgt.
18. Verfahren nach einem der Ansprüche 1 bis 17, dass zwischen Mobilfunknetzbetreiber und HBCI-Gateway-Betreiber ein Masterkey ausgetauscht wird.
19. Verfahren nach einem der Ansprüche 1 bis 18, dass eine zusätzliche Authentifikation des Teilnehmers über die Kennung seines Mobilanschlusses erfolgen, indem eine Auswertung der Calling-Line-Identification (CLI) erfolgt.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Nutzung von standardisierten Bankdienstleistungen über Mobilfunk, wobei die Datenübertragung zwischen einem Bankserver und einer Mobilstation auf dem HBCI-Übertragungsverfahren aufbaut. Problem dabei ist, dass das für das Internet konzipierte HBCI-Protokoll zu umfangreich für eine direkte Abbildung auf die heutige GSM-Mobilfunkwelt ist. Die Erfindung zeichnet sich dadurch aus, dass ein HBCI-Gateway in den Übermittlungsweg zwischen dem Bankserver und der Mobilstation geschaltet wird, der eine Transformation zwischen dem bankenseitig verwendeten HBCI-Übertragungsverfahren und einem auf der Mobilfunkseite verwendeten Übertragungsverfahren vornimmt.

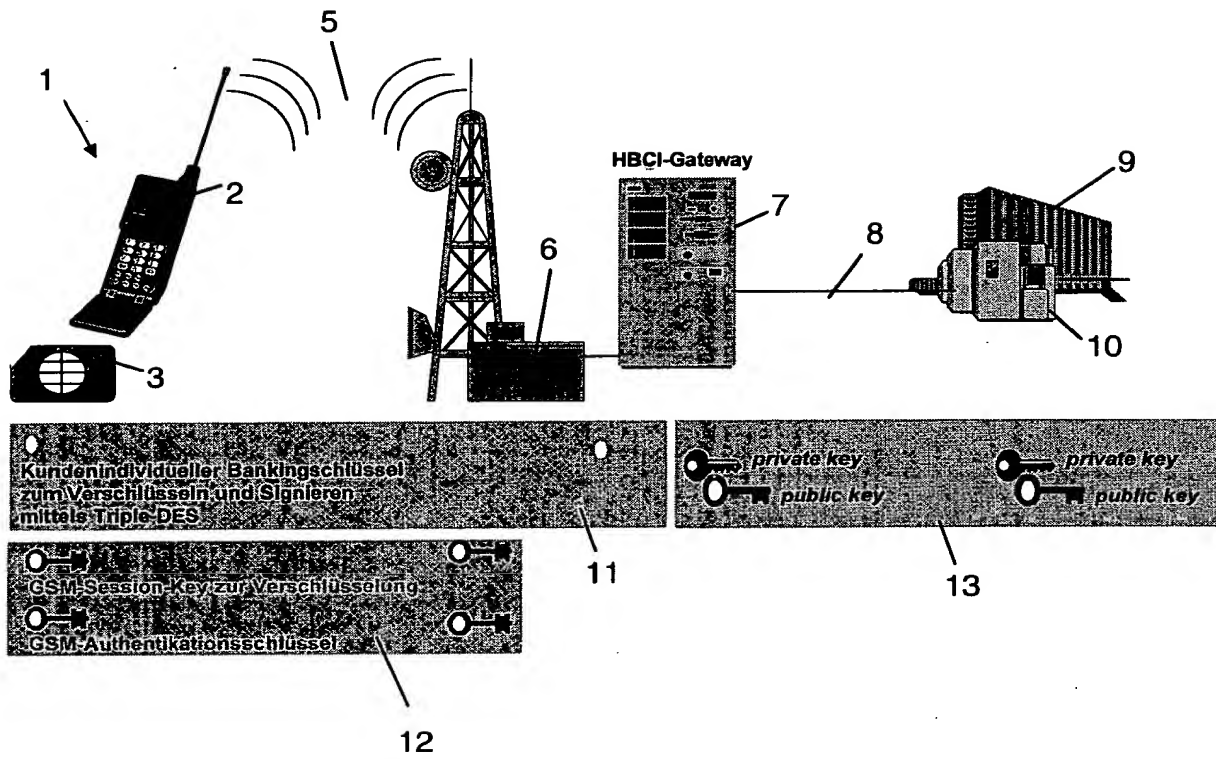
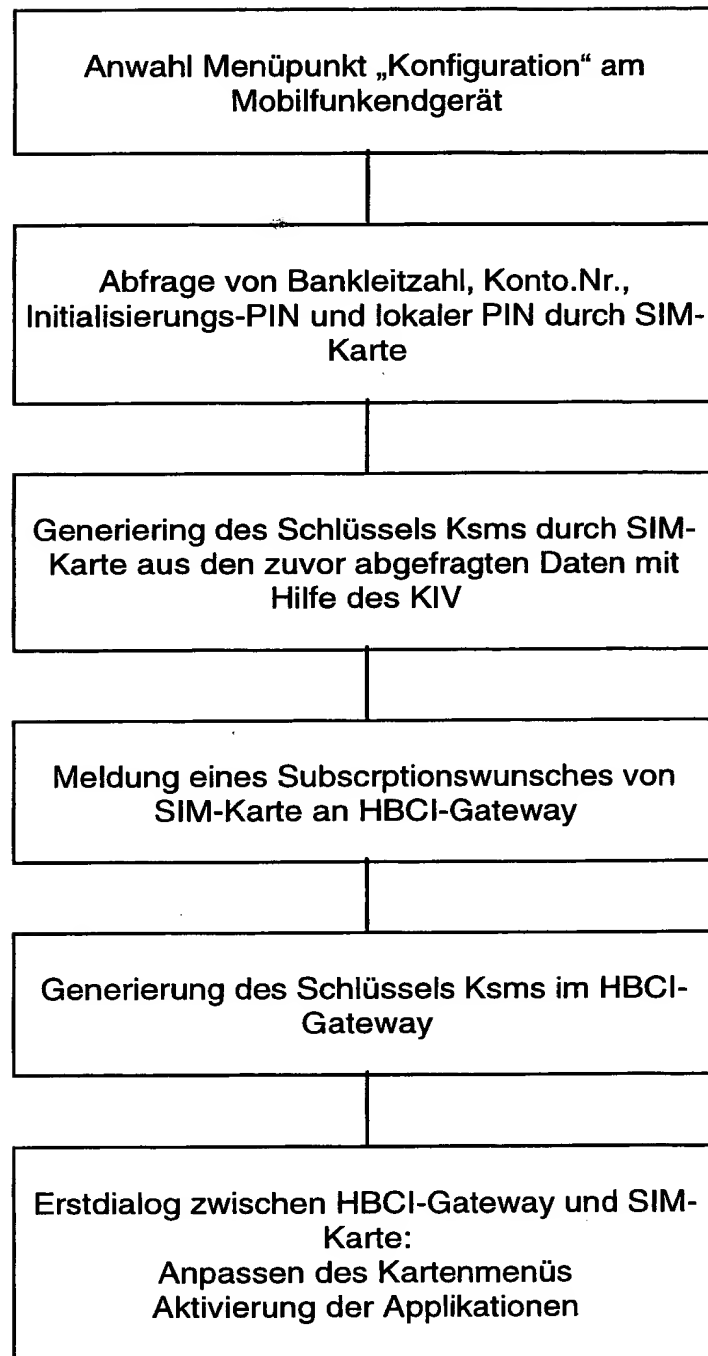


FIG. 1

Online-Subscription**FIG. 2**